UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,694	09/29/2000	Manav Mishra	42390P9326	1491

7590 05/03/2005

Libby N Ho
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 05/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/675,694	MISHRA ET AL.	
	Examiner	Art Unit	
	David Lazaro	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *30-52 and 54-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *30-52 and 54-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed 11/29/04.

2. Claims 1-29, 53 are canceled.

3. Claims 30, 31, 33-38, 54-56, 64, 65, 70 and 72 were amended.

4. Claims 30-52 and 54-73 are pending in this office action.

Claim Rejections - 35 USC § 102

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 30-52 and 54-73 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,772,333 by Brendel (Brendel).

7. With respect to Claim 39, Brendel teaches a method comprising: receiving a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session identifier (ID) (Col. 9 lines 57-65); determining if the transaction is a secure transaction (Col. 9 lines 57-63); determining if the session ID exists in a mapping table, if the transaction is a secure transaction (Col. 9 lines 63-67); and assigning a server to the user request and assigning a secure tunnel to the assigned server if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 - Note: The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

8. With respect to Claim 30, Brendel teaches all the limitations of Claim 34 and further teaches wherein assigning a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26 - Note: the secure tunnels are established as data is already being encrypted.).

9. With respect to Claim 31, Brendel teaches all the limitations of Claim 34 and further teaches the secure tunnel comprises a secure sockets layer (SSL) context (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

10. With respect to Claim 32, Brendel teaches all the limitations of Claim 31, and further teaches the SSL context comprises a source address, a destination address and an encryption algorithm (Col. 3 line 58 - Col. 4 line 25).

11. With respect to Claim 33, Brendel teaches all the limitations of Claim 39 and further teaches using a load balancing algorithm to assign a server to the user request if the transaction is not a secure transaction (Col. 9 lines 29-56).

12. With respect to Clam 34, Brendel teaches all the limitations of Claim 39 and further teaches subsequently receiving a second request comprising the session 1D; selecting the server corresponding to the session ID; and sending the second request to the selected server (Col. 10 lines 5-17).

13. With respect to Claim 35, Brendel teaches all the limitations of Claim 39 and further teaches wherein determining if the transaction is a secure transaction comprises determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

14. With respect to Claim 36, Brendel teaches all the limitations of Claim 39 and further teaches wherein a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58).

15. With respect to Claim 37, Brendel teaches all the limitations of Claim 39 and further teaches wherein a secure transaction comprises transactions in which personal data and credit card information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58)

16. With respect to Claim 38, Brendel teaches all the limitations of Claim 39 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

17. With respect to Claim 40, Brendel teaches all the limitations of Claim 39 and further teaches using a load balancing algorithm to assign the server to the user request (Col. 10 lines 5-17).

18. With respect to Claim 41, Brendel teaches all the limitations of Claim 39 and further teaches sending the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 lines 63 - Col. 10 line 4).

19. With respect to Claim 42, Brendel teaches all the limitations of Claim 39 and further teaches adding the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

20. With respect to Claim 43, Brendel teaches all the limitations of Claim 39 and further teaches wherein assigning a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26).

21. With respect to Claim 44, Brendel teaches all the limitations of Claim 43 and further teaches the secure tunnel comprises a secure sockets layer (SSL) context having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

22. With respect to Claim 45, Brendel teaches all the limitations of Claim 39 and further teaches wherein determining if the transaction is a secure transaction comprises determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

23. With respect to Claim 46, Brendel teaches 46 a method comprising: receiving a user request corresponding to a transaction (Col. 9 lines 29-37), the user request comprising a session identifier (ID) (Col. 9 lines 57-65); assigning a server to the user request (Col. 10 lines 5-17); determining if the transaction is a secure transaction (Col. 9 lines 57-63); assigning a secure tunnel to the assigned server if the transaction is a secure transaction (Col. 10 lines 5-17); adding the session ID, the server assignment, and the secure tunnel assignment as an entry to a mapping table if the transaction is a

secure transaction (Col. 10 lines 5-17 - The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

24. With respect to Claim 47, Brendel teaches all the limitations of Claim 46 and further teaches determining if the session ID exists in the mapping table, if the transaction is a secure transaction and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 4).

25. With respect to Claim 48, Brendel teaches all the limitations of Claim 46 and further teaches wherein assigning a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26).

26. With respect to Claim 49, Brendel teaches all the limitations of Claim 46 and further teaches the secure tunnel comprises a secure sockets layer (SSL) context having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

27. With respect to Claim 50, Brendel teaches all the limitations of Claim 46 and further teaches subsequently receiving a second request comprising the session ID; determining if the session ID exists in the mapping table; and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 17).

28. With respect to Claim 51, Brendel teaches all the limitations of Claim 46 and further teaches wherein a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58).

29. With respect to Claim 52, Brendel teaches all the limitations of Claim 46 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

30. With respect to Claim 57, Brendel teaches an article of manufacture including a machine-readable medium having stored thereon data representing sequences of instructions, which, when executed by a machine, cause the machine to perform operations including: receiving a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session identifier (ID) (Col. 9 lines 57-65); determining if the transaction is a secure transaction (Col. 9 lines 57-63); determining if the session ID exists in a mapping table, if the transaction is a secure transaction (Col. 9 lines 63-67); and assigning a server to the user request and assigning a secure tunnel to the assigned server if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 - Note: The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated

channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

31. With respect to Claim 54, Brendel teaches all the limitations of Claim 57 and further teaches using a load balancing algorithm to assign a server to the user request if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5 - 17).

32. With respect to Claim 55, Brendel teaches all the limitations of Claim 57 and further teaches adding the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

33. With respect to Claim 56, Brendel teaches all the limitations of Claim 57 and further teaches selecting from among a plurality of established secure tunnels with a plurality of server to assign a secure tunnel to the assigned server as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 and Col. 2 lines 9-26).

34. With respect to Claim 58, Brendel teaches all the limitations of Claim 57 and further teaches sending the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 lines 63 - Col. 10 line 4).

35. With respect to Claim 59, Brendel teaches all the limitations of Claim 57 and further teaches the secure tunnel comprises a secure sockets layer (SSL) context

having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

36. With respect to Claim 60, Brendel teaches an article of manufacture including a machine-readable medium having stored thereon data representing sequences of instructions, which, when executed by a machine, cause the machine to perform operations including: receiving a user request corresponding to a transaction (Col. 9 lines 29-37), the user request comprising a session identifier (ID) (Col. 9 lines 57-65); assigning a server to the user request (Col. 10 lines 5-17); determining if the transaction is a secure transaction (Col. 9 lines 57-63); assigning a secure tunnel to the assigned server if the transaction is a secure transaction (Col. 10 lines 5-17); adding the session ID, the server assignment, and the secure tunnel assignment as an entry to a mapping table if the transaction is a secure transaction (Col. 10 lines 5-17 - The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

37. With respect to Claim 61, Brendel teaches all the limitations of Claim 60 and further teaches determining if the session ID exists in the mapping table, if the transaction is a secure transaction and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 4).

38. With respect to Claim 62, Brendel teaches all the limitations of Claim 60 and further teaches subsequently receiving a second request comprising the session ID; determining if the session ID exists in the mapping table; and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 17).

39. With respect to Claim 63, Brendel teaches all the limitations of Claim 60 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

40. With respect to Claim 64, Brendel teaches a system comprising: a mapping table containing session identifiers (IDs) linked to server and secure tunnel assignments (Col. 9 line 63 - Col. 10 line 17); and a dispatcher to receive a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session ID (Col. 9 lines 57-65), to determine if the transaction is a secure transaction (Col. 9 lines 57-63), to determine if the session ID exists in the mapping table, if the transaction is a secure transaction(Col. 9 line 63 - Col. 10 line 17), and to send the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 10 line 5-17).

41. With respect to Claim 65, Brendel teaches all the limitations of Claim 64 and further teaches a load balancing table and wherein the dispatcher assigns a server to

the user request using the load balancing table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

42. With respect to Claim 66, Brendel teaches all the limitations of Claim 65 and further teaches the dispatcher adds the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 line 5-17).

43. With respect to Clam 67, Brendel teaches all the limitations of Claim 65 and further teaches the dispatcher determines if the transaction is a secure transaction by determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

44. With respect to Claim 68, Brendel teaches all the limitations of Claim 67 and further teaches a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58)

45. With respect to Claim 69, Brendel teaches all the limitations of Claim 65 and further teaches a quality of service (QoS) manager in communication with the dispatcher to decide which one of multiple user requests is processed if multiple user requests are sent to the same server (Col. 14 lines 11-18).

46. With respect to Claim 70, Brendel teaches a system comprising: a load balancing table (Col. 10 lines 5-17); a mapping table containing session identifiers (IDs) linked to server and secure tunnel assignments (Col. 9 line 63 - Col. 10 line 17); and a dispatcher to receive a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session ID (Col. 9 lines 57-65), to determine if the transaction is a secure transaction (Col. 9 lines 57-63), to determine if the session ID exists in the

mapping table, if the transaction is a secure transaction (Col. 9 line 63 - Col. 10 line 17), and to assign a server to the user request using the load balancing table and a secure tunnel to the assigned server if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

47. With respect to Claim 71, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher further assigns a server to the user request using the load balancing table if the transaction is not a secure transaction (Col. 9 lines 37-56).

48. With respect to Claim 72, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher further selects the secure tunnel from among a plurality of established secure tunnels with a plurality of established servers, if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 and Col. 2 lines 9-26).

49. With respect to Claim 73, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher further adds the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

Response to Arguments

50. Applicants' arguments filed 11/29/04 have been fully considered but they are not persuasive.

51. Applicants argue on page 12 of the remarks - "*In claim 39, a secure tunnel is assigned to the assigned server. There is no suggestion in Brendel that the load balancer should assign secure tunnels. Instead, the server would appear to be*

responsible for selecting and establishing the SSL session. This puts more load on the server and raises the possibility of conflicts between simultaneous secure tunnels at a single server farm."

a. The examiner first notes that in claim 39, there is no associated entity that performs any of the assigning function. Furthermore the claim language does not state anything about selecting and establishing an SSL session, nor does the claim language discuss simultaneous secure tunnels.

b. In regards to the Brendel reference, the server to which the client is ultimately connected is not selected by the server as applicants assert. It is instead assigned/selected by the load-balancer. Brendel states in col. 9 lines 31-34, "The load-balancer is activated when a connection is received by the web farm from the network. The load-balancer parses the incoming request data for a SSL session ID field, step 82." (emphasis added). Found session ID's are compared to a stored table of session ids (Col. 9 lines 63-65). This table is clearly in the load-balancer according to Col. 9, lines 1-12. Col. 10 lines 5-17 then describes that when no matching SSL session ID is found in the table, the load balancer is capable of assigning a server to the user request and further associating the assigned server with an SSL session ID (Col. 10 lines 5-17). The examiner considers this association to be within the scope of "assigning a secure tunnel to the assigned server" (as from claim 39). This is in part based on the interpretation noted by the examiner in the rejection wherein a tunnel can be a designated channel of communication (as stated in applicant's specification on page 6, line 26). The connection to the assigned server (the SSL session

corresponding to the SSL session ID) is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel.

52. Applicant's argue on page 12 of the remarks - *"The Examiner suggest that a secure tunnel is a designated channel of communications that is encrypted. This suggestion ignores whether the secure is assigned and tracked at the respective servers as in Brendel or by the dispatcher as recited in the claims."*

c. As explained already, the servers of Brendel do not do the assigning. The load-balancer of Brendel does this function. Furthermore, only claim 70 recites the dispatcher as specifically performing such a function. The examiner interprets the load-balancer of Brendel to be within the scope of a dispatcher and as argued above, is capable of "assigning a secure tunnel to the assigned server".

Conclusion

53. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 571-272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

David Lazaro
April 22, 2005

ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100